LA-UR-04-4321

Approved for public release; distribution is unlimited.

Title: **AN APPLICATION OF UNATTENDED AND REMOTE MONITORING TO SENSITIVE SYSTEMS**

Author(s): **D. G. Langner and D. W. MacArthur**

Submitted to: **45th Annual INMM Meeting
Orlando , FL
July 18 -22, 2004
(INMM Paper)**

Los Alamos
NATIONAL LABORATORY

LAUR-04-xxxx

An Application of Unattended and Remote Monitoring to Sensitive Systems

Diana G. Langner and Duncan W. MacArthur
Los Alamos National Laboratory
Los Alamos, NM 87545 USA
505/667-2874

Abstract

Unattended and remote monitoring has proven to be an effective way to reduce the cost of inspection activities as well as the impact of inspections on a facility. Recently, remote transmission of data over the internet has become more cost effective and is an attractive option to reduce travel to a facility and thus further reduce costs. In some cases, however, the data collected by these systems is deemed classified or sensitive by the host country and under such circumstances the data cannot be transmitted. This is a type of catch-22 situation where the host country may have acceptable means to transmit classified data, but that means is itself classified and cannot be shared.

Unattended systems sometimes fail and after such a failure an inspector may discover that months of safeguards information has been lost. If state-of-health information can be remotely transmitted such a failure can be detected in a more timely manner and less data will be lost. When classified data are involved, however, a host may be reluctant to allow the transmittal of this type of information because of the potential that this transmission route could provide unauthorized access to the sensitive data. In this paper we will discuss an application of the information barrier concept that may allow an inspector to have access to information from the unattended system while giving the host assurances that no classified data are being transmitted.

Introduction

The basic concept of an information barrieris illustrated in Figure 1. [1-5]. A measurement system that collects data of a sensitive nature is encapsulated by a barrier that protects the information and only allows unclassified data through. A control element of the system provides any necessary external input to the measurement system as well as monitoring and maintaining the security of the system. Both control input and any output from the system are limited to assure that no sensitive information can be compromised. This is usually accomplished by minimizing the number of bits of information that is passed through the barrier. Finally, the data barrier assures that only one-way communication is possible—that is an input channel cannot be used for output and vice versa.

This work is supported by the United States National Nuclear Security Administration's International Safeguards Office.

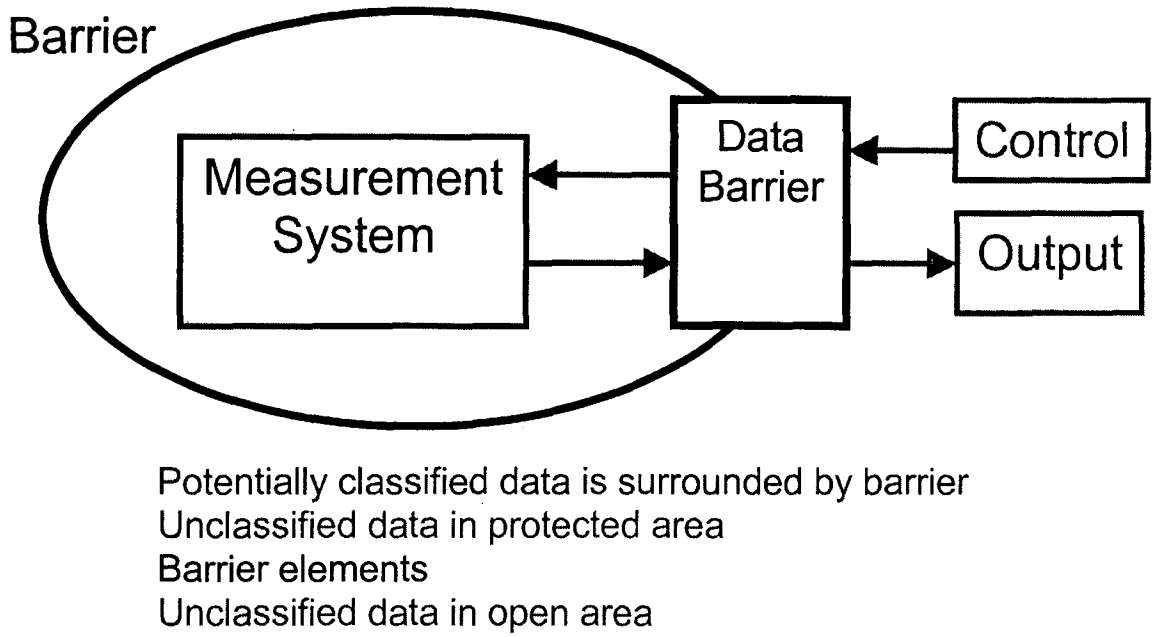

Figure 1. The basic information barrier concept.

To date, the information barrier concept has been applied to and successfully demonstrated with attribute measurement systems. [2, 4, 5] These systems are conventional non-destructive assay measurement systems whose outputs are compared to an agreed threshold and only simple yes/no results are passed through the barrier. These systems protect the classified information from unauthorized disclosure while giving the inspector confidence that the system is operating nominally. In this paper, we will explore the idea of using information barriers to protect information in systems for which it would be desirable to remotely monitor the data from the measurement system but for which legal constraints forbid such transmission.

Unattended and Remote Monitoring

Many of the advantages of unattended and remote monitoring systems have been realized. A system that can operate in an unattended mode without the loss of safeguards data and that can transmit that data to an inspector in a central location results in considerable cost savings relative to inspector travel and on-site presence. Such systems also benefit the facility operator by reducing the disruption to normal operations caused by inspection activities. Unattended systems have been used for many years. It is only recently that remote transmission of data has become cost effective enough to be practical.

Great strides have also been made in developing methods to protect data during remote transmission. Virtual Private Networks (VPNs), in particular, are gaining wide acceptance as a secure way to transmit even some forms of sensitive data. In some instances, however, a host country may be constrained by its own laws that forbid the remote transmission of

data that it deems to be sensitive or classified. Examples of data that might be so constrained are data that reveal the location and amounts of special nuclear materials in a given inventory at a given time and data that reveal the details of a nuclear facility such as the location of physical security devices or methodologies employed during security exercises. The host country may have internal mechanisms for the remote transfer of such data—but these mechanisms may themselves be classified and cannot be shared with an inspector. In such cases, the application of the information barrier concept may provide a means to remotely access some or even all of these data. Such applications do not circumvent the need to secure the remote communication by some means such as a VPN.

Application of the Information Barrier Concept to State-of-Health Information

There are two types of information from an unattended system that are important to an inspector—the data that the system is collecting and information concerning the state-of-health of that system. Unattended systems have historically taken data and stored that data for some interval of time that corresponds to the periodic collection of the data by the inspector for review. If during that time interval the system suffers a failure, the inspector has not known about it until he or she returns to the facility to collect the data. If the failure is catastrophic, safeguards data are lost, and difficult and expensive measures are often required to regain the data. The consequences of such failures can be mitigated by building redundancy into a system, but this can be expensive.

One application of the information barrier concept for such systems is to only remotely transmit a state-of-health message to the inspector so that if a system is starting to fail, there can be a more rapid response to avoid loss of safeguards data. Figure 2 shows an example of this concept.

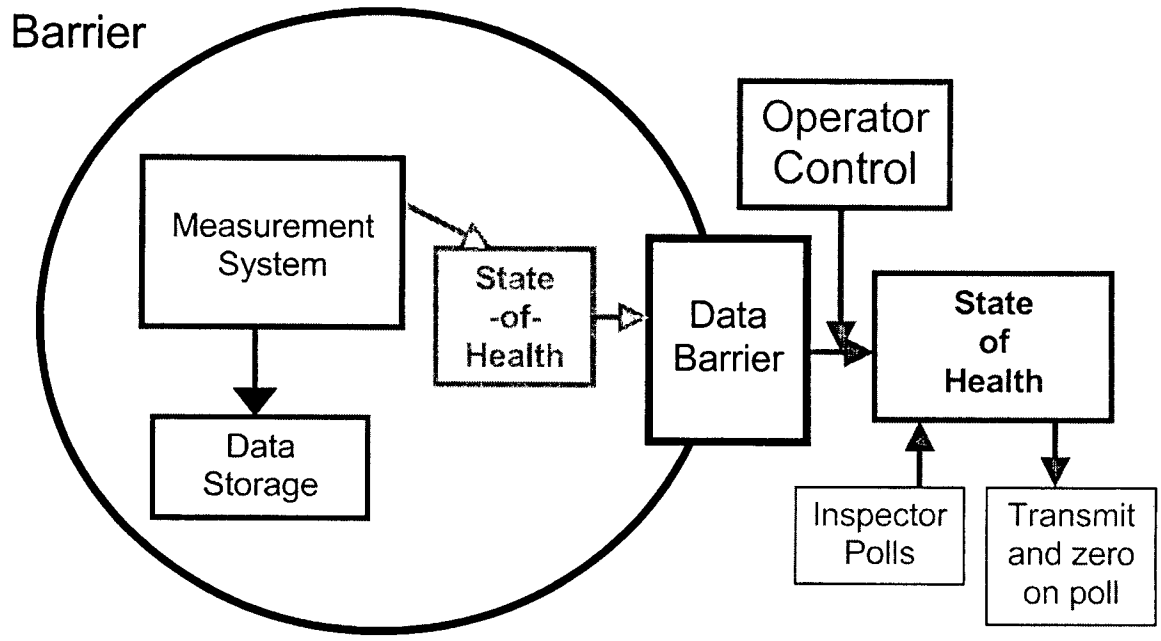

Figure 2. Unattended system with state-of-health transmission only.

In this example, the barrier may be the usual inspector-owned, tamper-indicating rack that houses the electronics for the unattended system. For most systems of this type, the data inside the rack are available to the inspector when he or she is onsite, but the host forbids remote transmission of these data. A first step is for the operator and inspector to negotiate an acceptable data transmission rate for the state-of-health information. The rate of data transmission that is acceptable can depend on several factors – the amount of data that are required to reveal sensitive information and the confidence that both the host and inspectorate have that this channel is secure and reliable.

Such state-of-health information could be simply a 1-bit – "I'm OK/ I'm not-OK" message or a negotiated error code of two or more bits. If both parties are confident that only state-of-health information can be delivered via this route, this information could be delivered frequently to the data barrier and then delivered to a buffer that could be remotely polled and zeroed by the inspector. If there is concern that sensitive information could be surreptitiously diverted through the state-of-health channel, an operator controlled clock could be used to control the rate at which the data are delivered to the buffer. The operator may want an additional control to be able to turn-off the connection to the output buffer in case an off-normal event occurs. Because the inspector polls and zeros the buffer, the inspector would also know when the operator disconnected the state-of-health information and could respond accordingly.

Application of the Information Barrier Concept for Time Sensitive Information

Some types of data are time-sensitive. As an example, video surveillance of a facility may reveal the current security posture of the facility or sensitive operations happening at the facility. These data may not be sensitive after a certain time period has elapsed. In such an example, the application of the information barrier concept may require that the unattended system store the data for an agreed period of time and then transmit it. In this case, state-of-health information will also be important to the inspector so that there is confidence that the system is operating normally while the data are being held back. This concept is shown in Figure 3.

In this example, state-of-health information is treated as in the case above, but now there is a time delay before data is transmitted through the data barrier. In this case, it will likely be desirable to build this delay with some kind of security watchdog function to assure that the delay cannot fail and reveal classified information. This security watchdog circuit could terminate transmission to the data barrier if the time delay function failed.

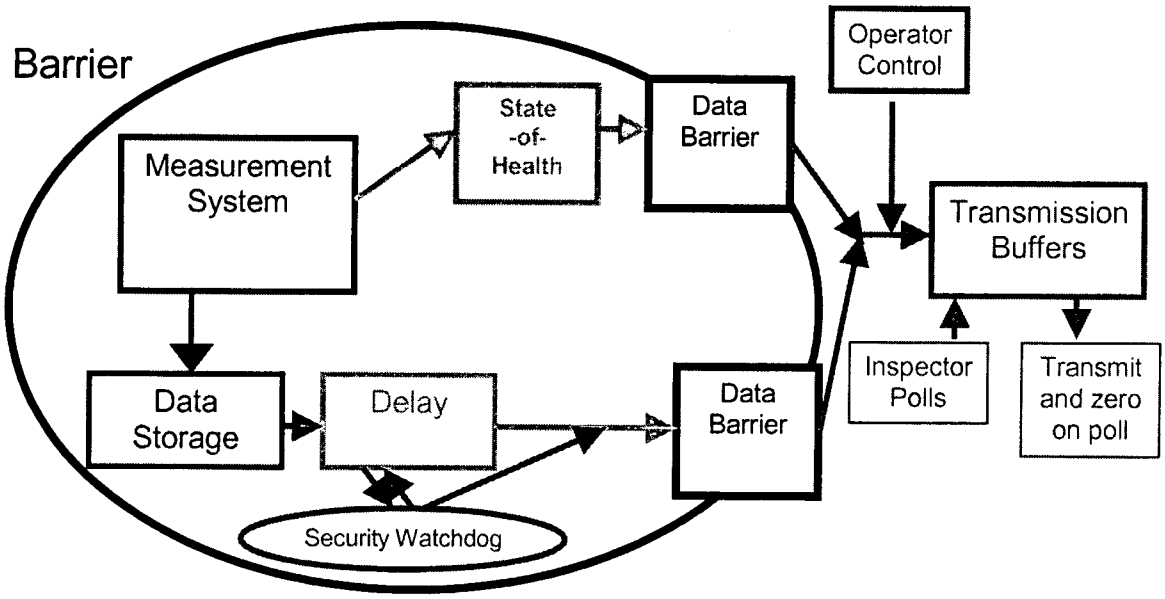

Figure 3. Information Barrier Concept for Time Sensitive Information

Application to Inventory Verification

The application of the information barrier concept to inventory verification systems for which the inventory information is sensitive would be very similar to existing applications for attribute measurement systems. Figure 4 gives an example.

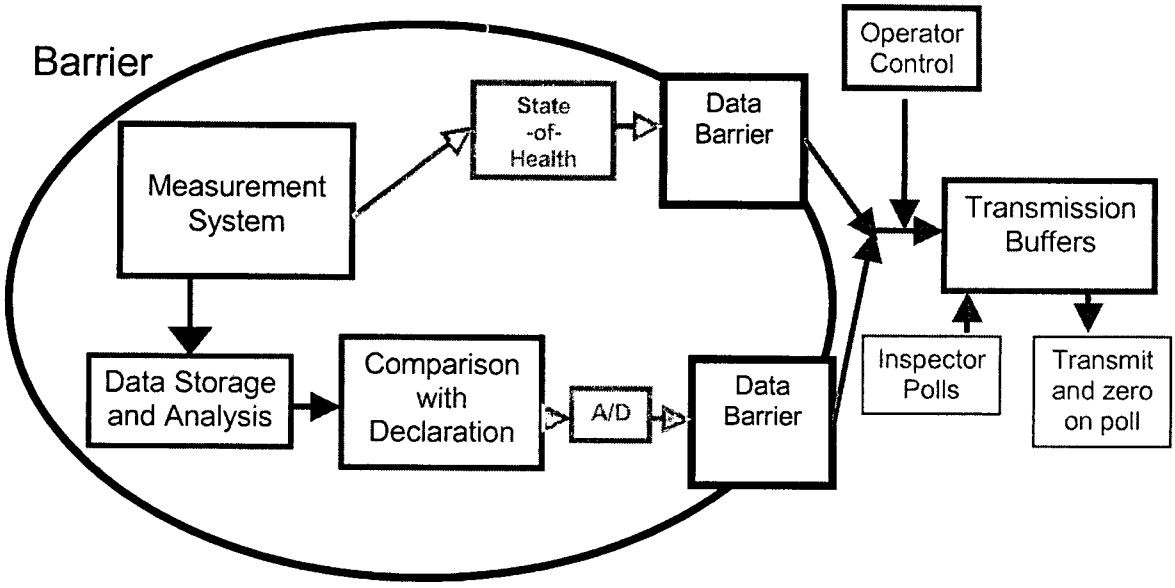

Figure 4. Information barrier concept for inventory verification

This example presents some new challenges. First, the declaration information must be input to the system. The operator controls this information, but the inspector must be

assured that in putting this information into the system, the inspection system itself is not compromised. For static inventories, this operation could be done in batch mode using a ROM chip, for example, with the inspector present. For non-static inventories, this is more difficult. A "mailbox" method where the system retrieves the information through a data barrier from an operator buffer may be a solution. It would be important in this case that the system "pulls" this data rather than the operator "pushing" it, to have confidence that this outside data is not compromising the inspection system itself. Second, the measurement data must be compared to the declaration and put into some unclassified form for transmittal. The form chosen would need to be negotiated between host and inspectorate. One form would be to transmit a comparison of the "Assay" result to the declaration. Such a ratio with associated statistical information would give the inspector a great deal of information about system performance relative to bias and precision. Another way to transmit results would be using a simple pass/fail.

Conclusions

The information barrier concept may provide a tool for the handling of sensitive data and preconditioning of that data that will allow the remote transmission of information valuable to the inspector. In particular, the application of the information barrier concept so that state-of-health information can be transmitted with confidence that no sensitive information is compromised will reduce the risk of loss of safeguards data. If the information to be protected is time sensitive, the concept can provide a means to delay transmittal until the information is no longer sensitive and to assure that the delay is adequate to protect the sensitive information. Finally, the concept may also be applicable to inventory verification systems if the inventory results can be reduced to an unclassified form by comparison with pre-stored inventory data or data supplied using a mailbox concept.

References

[1] D. A. Close, D. W. MacArthur, and N. J. Nicholas, "*An early Version of an Information Barrier,*" *Journal for Nuclear Materials Management*, Volume XXXI, No. 1, p 53 – 58, Fall 2002.

[2] Diana Langner, Robert Landry, Sin-Tao Hsue, Duncan MacArthur, Doug Mayo, Morag Smith, Nancy Jo Nicholas, Rena Whiteson, Thomas B. Gosnell, Zachary Koenig, S. John Luke, James Wolford, *"Attribute Measurement Systems Prototypes and Equipment in the United States,"* Proceedings of the INMM 42nd Annual Meeting, Indian Wells, CA, July 15-19, 2001

[3] Duncan W. MacArthur, Rena Whiteson and James K Wolford, Jr., *"Functional Description of an Information Barrier to Protect Classified Information,"* proceedings of the INMM 40th Annual Meeting, Phoenix, AZ, July 25-29, 1999.

[4] Duncan W. MacArthur and Diana Langner, "*Attribute Verification Systems: Concepts and Status,*" proceedings of ESARDA 2003, Stockholm, Sweden, May 13-15, 2003.

[5] John M. Puckett, Diana Langner, Sin-Tao Hsue, Duncan MacArthur, Nancy Jo Nicholas, Rena Whiteson, Thomas B. Gosnell, Zachary Koenig, James Wolford, Massimo Aparo, Juri Kulikov, Julian Whichello, Valery J. Poplavko, Sergei Feodorovitch Razinkov, Dmitriy S. Semenov, Vladimir Terekin, *"General Technical Requirements and Functional Specifications for an Attribute Measurement System for the Trilateral Initiative,"* Proceedings of the INMM 42nd Annual Meeting, Indian Wells, CA, July 15-19, 2001.